WORTH READING

Supplying War:
Logistics from Wallenstein to Patton

Martin van Creveld
Cambridge University Press, 1977

Reviewed by Geoffrey French, a Counterintelligence Analyst with General Dynamics and former Logistics Specialist for the U.S. Marine Corps Reserve.

The typical image of Napoleon is not one where he remains 60 miles behind his advancing troops, personally overseeing the army's supplies. Nor does the thought of the Prussian army in 1870 usually conjure images of thousands of soldiers gathering the harvest around Paris, processing and distributing food. Yet these images would be historically accurate. The study of logistics is often an afterthought, but to armies in the field, it is of paramount importance, and often, as in the two instances illustrated above, becomes the single most important task the military must address. Martin van Creveld — a renowned historian whose works have been used to educate U.S. Army and Marine Corps officers — brings logistics to the forefront in this military classic, *Supplying War: Logistics from Wallenstein to Patton*.

Just as the instances above may change the reader's notions of how two great militaries actually functioned, van Creveld challenges a number of ideas perpetuated in military history. His book describes campaigns in five military periods: 17th and 18th century warfare, Napoleonic warfare, the Franco-Prussian War, and World Wars I and II. In each, he uses detailed accounts of food, ammunition, transportation, requests and deliveries to study "the practical art of moving armies and keeping them supplied."

In this way, van Creveld wins his first victory. Whereas others who address logistics tend to rely on theories and concepts, van Creveld thoroughly documents the seemingly mundane to craft well-supported arguments about the feasibility of certain campaigns or retrospective criticisms (such as the *Schlieffen Plan* and critics of Moltke's changes). This makes his arguments — such as after the immediate mobilization, the railroads provided no advantage to the Prussians in 1870 because the supplies delivered to the railheads could not then be transported to the troops in the field — very convincing.

Van Creveld's writing style makes his ideas easy to absorb. Each chapter is highly organized, describing the commonly held thoughts of the era he is about to explore and the methods he will use to examine them. In each, he reviews salient points and draws conclusions from the research. This said, van Creveld assumes a working knowledge of military history. Those familiar with the battles he explores will get much out of his work. Those who are not students of military history may need a supplementary text to describe the strategy, maneuver and tactics of the battles, which are of secondary importance in this particular study.

Supplying War validates the importance of logistics to those who work at it daily. It is important for them, therefore, to use this book as a way of getting a firm understanding of the role logistics has played in military history. For those involved in military strategy, it is equally important. Van Creveld shows that inattention to logistical considerations have undone many commanders in the past. If military success rides on taking risks when opportunities present themselves, *Supplying War* shows that commanders can only take those risks if they have already addressed operational logistics.

The Next War Zone
Confronting the Global Threat of Cyberterrorism

James F. Dunnigan
Citadel Press, 2002

Reviewed by Scott Curthoys, a Counterintelligence Analyst contracted to a federal law enforcement agency and retired Army military intelligence and foreign area officer.

The prognosticators of cyberterrorism were wrong this time. By their reckoning, the war in Iraq should have resulted in major computer attacks against the United States. It was, after all, if not an appropriate time for a

symbolic and devastating "digital Pearl Harbor," then certainly the right time for smaller cyber-attacks against electric power distribution, transportation networks and banks. Despite the fact that the number of defaced Web sites increased significantly over prewar levels, no second front in cyberspace was ever opened.

This lack of a cyberwar, however, does not translate into the absence of threats to U.S. computer systems. Similarly, it does not mean that U.S. computer systems are not vulnerable. But it does raise questions about how extensive is the threat and what would be the impact of a serious cyber-attack? In his book *The Next War Zone*, James Dunnigan attempts to answer these questions by describing the battlefield, identifying the warriors and putting forth his ideas on how to survive what he envisions to be the coming cybercataclysm.

Dunnigan has taken on a daunting task. In addition to personal computers (PCs), there are thousands of computer systems that most Americans never hear about, such as process control systems or supervisory control and data acquisition systems that electronically oversee water systems, electric grids, railroad switches and other components of America's infrastructure. Despite the ubiquitous and benign nature of computers in our lives, many people are still mystified by how they work, how they connect with each other and how they can be threatened from great distances.

Dunnigan tries to bridge this knowledge gap by introducing the reader to the concept of cyberwar and how this emerging warfare method affects the average American. He does this by sequencing the chapters in his book to take the reader through an introduction to cyberwar, its history and components, and finishes with a hopeful chapter titled "Surviving Cyberwar." While the book's organization is sound, it is difficult to cut through Dunnegan's shrill rhetoric and find a reasoned and consistent description of who or what is threatening the United States.

The Next War Zone is straightforward in its theme: there is a real threat of a cyber-attack against the United States; the United States is vulnerable to such an attack; and the impact of such an attack could be very grave. The book's premise is based on the thought that the United States is a digitally homogeneous society. It is not. There are millions of networks, some linked with others through the Internet or private nets, some not linked at all, and each with different vulnerabilities. Unless coupled with a physical attack on key assets, a digital attack on one of these networks, or even several large networks, will not likely have a devastating impact on the United States. In making his argument, Dunnigan cannot escape the hyperbole and misconceptions that usually characterize discussions by subject matter experts on this topic.

The assertion that a cyber-attack can alter the orbits of satellites belies a lack of understanding of satellite telemetry, tracking and control, as well as the digital security that surrounds these national assets. The author makes several unsubstantiated assertions that "Cyberwarfare is a battle for control of the Internet ... " (the Internet is not something that can be occupied and defended as if it were the objective in a digital king-of-the-hill game); and that banks, big corporations and large Web sites have the resources to protect themselves from cyber-attack, but PC users and small businesses don't, leaving them as potential cybertargets.

The clearer understanding and more careful use of relevant terms and definitions might have restrained the author's use of "bogeyman" tactics. However, the author fails in this aspect as well. Dunnigan ignores extant doctrinal concepts over what constitutes information operations, information warfare and cyberwar. In chapter two he refers to Alexander the Great as a cyberwarrior because he attempted to control what was released to the media of the day. This muddles the concept of cyber — having to do with digitized information communicated over computer networks — and contradicts his own definition of cyberwarrior presented on page one.

Perhaps the biggest frustration with *The Next War Zone* is its total absence of footnotes, endnotes or a bibliography. This absence of references is indeed odd coming from an experienced author and part-time television analyst. The reader should meet the author's request for faith, as well as his dramatic prose, with extreme skepticism.

Correction

In the September-October 2003 *Army AL&T* article, "FY04 LTC/GS-14 PM/AC Slate," LTC Dwayne A. Morton should have been listed as becoming Product Manager for Test, Measurement and Diagnostic Equipment. We regret this error.